Groupe des permutations d'un ensemble fini. Applications.

1 Groupe des permutations d'un ensemble fini

1.1 Présentation du groupe symétrique

Définition 1 Soit E un ensemble fini de cardinal n. L'ensemble des bijections de E dans E muni de la composition est un groupe de permutations fini appelé *groupe symétrique d'ordre n* et noté $\mathfrak{S}_n$.

Théorème 1 Si E est un ensemble fini de cardinal $n > 0$, $\mathfrak{S}_E$ ne dépend,à un isomorphisme près, que de l'entier n.

Théorème 2 (de Cayley) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Définition 2 Soit $\sigma \in \mathfrak{S}_n$. La *signature* de σ notée $\varepsilon(\sigma)$ est définie par $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$.

Proposition 1 Pour $n \geqslant 2$, la signature est un morphisme de groupe surjectif de $\mathfrak{S}_n$ dans $\{-1; 1\}$.

Définition 3 On appelle *groupe alterné* et on note $\mathfrak{A}_n$ le noyau $\mathrm{Ker}(\varepsilon)$ où ε est l'homomorphisme de $\mathfrak{S}_n$ dans $\{-1; 1\}$: $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = 1\}$.

Proposition 2 $\#\mathfrak{S}_n = n!$ et $\#\mathfrak{A}_n = \frac{n!}{2}$

1.2 Les générateurs de $\mathfrak{S}_n$ et leurs propriétés

1.2.1 Définitions

Définition 4 Soit $G =< \sigma >$ le groupe cyclique engendré par $\sigma \in \mathfrak{S}_n \backslash \{Id\}$. G opère sur $E = [\![1; n]\!]$ par $(\sigma, x) \in G * E \mapsto \sigma(x)$. On dit que σ est un *cycle* si pour l'opération de G sur E, il existe une orbite et une seule non réduite à un seul élément.

Définition 5 Le cardinal de l'orbite non réduite à un seul élément d'un cycle est appelé *longueur* du cycle.

Définition 6 L'orbite de cardinal supérieur à 2 d'un cycle σ est appelé *support* de σ et noté $supp(\sigma)$.

Définition 7 On appelle *transposition* un cycle de longueur 2.

Définition 8 (équivalente) Une transposition de $\mathfrak{S}_n$ est un élément $\tau \in \mathfrak{S}_n$ tel que $\tau(i) = j, \tau(j) = i$ et $\tau(k) = k$ pour $k \notin \{i, j\}$ avec $i, j \in [\![1; n]\!]$; $i \neq j$.

Remarque 1 La signature d'une transposition est -1 ; celle d'un cycle de longueur k est $(-1)^{k+1}$.

1.2.2 Décomposition en cycles disjoints

Théorème 3 Toute permutation de $\mathfrak{S}_n$ se décompose en produit fini de cycles à supports disjoints deux à deux. Cette décomposition est unique à l'ordre près des facteurs.

Corollaire 1 $\mathfrak{S}_n$ est engendré par ses cycles. $\mathfrak{A}_n$ est engendré par ses cycles de longueur 3.

Théorème 4 Tout cycle se décompose en produit de transpositions.

Corollaire 2 $\mathfrak{S}_n$ est engendré par ses transpositions.

Remarque 2 On en déduit que la signature est l'unique morphisme de groupe surjectif de $\mathfrak{S}_n$ dans $\{-1;1\}$.

1.2.3 Propriétés

Lemme 1 La longueur d'un cycle sur un ensemble fini E est égal à son ordre dans $\mathfrak{S}_E$.

Théorème 5 Si $\sigma = \sigma_1 \circ \cdots \circ \sigma_n$ où les σ_i sont des cycles à support disjoints de $\mathfrak{S}_n$ alors l'ordre de σ dans $\mathfrak{S}_n$ est le ppcm des ordres des σ_i.

Lemme 2 Deux cycles sont conjugués si et seulement si ils ont même longueur.

Théorème 6 Deux eléments de $\mathfrak{S}_n$ sont conjugués si et seulement si pour tout $l \in [\![1;n]\!]$ le nombre de l-cycles apparaissant dans leur décomposition en cycles disjoints est le même.

1.3 Propriétés de quelques sous-groupes du groupe symétrique

1.3.1 Le groupe alterné

Théorème 7 Pour $n \geqslant 5$ le groupe $\mathfrak{A}_n$ est simple. (ie ses seuls sous groupes distingués sont lui-même et l'identité).

Théorème 8 $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$ pour tout n.
Pour $n \geqslant 5$, c'est avec $\mathfrak{S}_n$ et $\{Id\}$ le seul sous-groupe distingué de $\mathfrak{S}_n$.

1.3.2 Autres sous groupes

Théorème 9 Pour $n \geqslant 3$ le centre de $\mathfrak{S}_n$ (ie l'ensemble des éléments de $\mathfrak{S}_n$ qui commutent avec tous les autres) est trivial (ie réduit à $\{Id\}$).

Théorème 10 Pour $n \geqslant 2$ $D(\mathfrak{S}_n) = \mathfrak{A}_n$ et pour $n \geqslant 5$ $D(\mathfrak{A}_n) = \mathfrak{A}_n$ où $D(G) = \{xyx^{-1}y^{-1} | x, y \in G\}$ est le groupe dérivé de G.

Théorème 11 Les sous-groupes d'indice n de $\mathfrak{S}_n$ sont isomorphes à $\mathfrak{S}_{n-1}$.

2 Applications

2.1 Les isométries et le groupe symétrique

Théorème 12 Les groupes d'isométries positives du tétraèdre sont isomorphes à $\mathfrak{A}_4$; celles du cube et de l'octaèdre à $\mathfrak{S}_4$ et celles de l'isodécaèdre et du dodécaèdre à $\mathfrak{A}_5$.

Théorème 13 Les groupes d'isométries du tétraèdre sont isomorphes à $\mathfrak{S}_4$; celles du cube et de l'octaèdre à $\mathfrak{S}_4 \times \{Id; -Id\}$ et celles de l'icosaèdre et du dodécaèdre à $\mathfrak{A}_5 \times \{Id; -Id\}$.

2.2 Résolution d'équations

Définition 9 Un groupe G est dit *résoluble* lorsqu'il existe une chaîne de sous-groupe $\{e\} = U_0 \subset \ldots \subset U_k = G$ $(k \in \mathbb{N})$ vérifiant pour tout $i \in [\![0; k-1]\!]$ les propriétés : (1) U_i est un sous-groupe distingué de U_{i+1} (2) le groupe quotient U_i/U_{i+1} est commutatif

Théorème 14 Pour $n \geqslant 5$ $\mathfrak{S}_n$ n'est pas résoluble (et $\mathfrak{A}_n$ non plus).

Définition 10 Soit E le corps de décomposition du polynôme $P(X) \in K[X]$. On appelle *groupe de Galois du polynôme* $P(X)$ l'ensemble des automorphismes de E tels que restreints à K ils soient l'identité.

Théorème 15 Le groupe de Galois du polynôme unitaire général de degré n (ie de la forme $X^n + u_{n-1}X^{n-1} + \ldots + u_1X + u_0 \in K(u_0, \ldots, u_{n-1})[X]$) est isomorphe à $\mathfrak{S}_n$.

Définition 11 Une équation est dite *résoluble par radicaux* si son corps des racine $L = K(\alpha_1, \ldots, \alpha_n)$ est une extension de K par radicaux ie s'il existe une suite finie d'extensions simples : $K = K_0 \subset K_1 \subset \ldots \subset K_s = L$ telles que $K_{i+1} = K(\alpha_i)$ et $\alpha_i^{n_i} = b_i \in K$.

Théorème 16 Si l'équation générale de degré n (ie l'équation $P(X) = 0$ où P est le polynôme unitaire général de degré n) est résoluble par radicaux alors le groupe de Galois de P est résoluble. On note que ceci revient à avoir $\mathfrak{S}_n$ résoluble.

Corollaire 3 (Théorème d'Abel) L'équation générale de degré n sur un corps de caractéristique nulle n'est pas résoluble par radicaux pour $n \geqslant 5$.

2.3 Applications antisymétrisées et Déterminants

Théorème 17 Soit E un K-ev (avec K corps commutatif et $car(K) \neq 2$). Soit $\mathscr{L}_p(E)$ l'ev des formes p-linéaires sur E. Le groupe symétrique opère sur $\mathscr{L}_p(E)$ par $(\sigma, f) \in \mathfrak{S}_n \times \mathscr{L}_p(E) \mapsto \sigma * f$ où $\sigma * f : E^p \to K,\ (x_1, \ldots, x_p) \mapsto f\left(x_{\sigma(1)}, \ldots, x_{\sigma(p)}\right)$.

Définition 12 Soit E K-ev, $p \in \mathbb{N}, f \in \mathscr{L}_p(E)$. f est *antisymétrique* ssi $\forall \sigma \in \mathfrak{S}_p, \sigma * f = \varepsilon(\sigma) f$

Théorème 18 f est antisymétrique ssi $\forall \tau \in \mathfrak{S}_p, \tau * f = -f$

Définition 13 Soit $f \in \mathscr{L}_p(E)$. On appelle *antisymétrisée de* f et on note $Af = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon(\sigma)\sigma * f$.

Proposition 3 Af est une forme p-linéaire antisymétrique.

Théorème 19 Soit K un corps, $Car(K) \neq 2$, E K-ev de dimension n, $B = \{e_1, \ldots, e_n\}$ base de E, $B^* = \{u_1, \ldots, u_n\}$ une base duale. Alors $f : E^n \to K, (x_1, \ldots, x_n) \mapsto \prod_{i=1}^{n} u_i(x_i)$ est une forme n-linéaire sur E. On a $\det_B = Af$.

Théorème 20 L'espace vectoriel des formes n-linéaires alternées sur E (où $\dim(E) = n$) est de dimension 1. Si $B = \{e_1, \ldots, e_n\}$ base de E, alors $\forall f \in \mathscr{L}_n(E)$ alternée $f = f(e_1, \ldots, e_n) \det_B$.

Remarques

Attention, j'ai choisi de ne pas ou peu parler de :
- groupes diédraux
- polynomes symétriques
- liens entre certains groupes symétriques et certains groupes linéaires
- automorphismes intérieurs
- classes de conjugaisons

Bibliographie

[1] Jean-Marie Arnaudiès. *Les cinq polyèdres réguliers de* $\mathbb{R}^3$ *et leurs groupes*. Polycopié.

[2] Jean-Marie Arnaudiès et Henri Fraysse. *Cours de Mathématiques — 1*, volume Algèbre. Dunod, 1987.

[3] M. Lesieur. *Groupes finis*. Recueil de notes prises par les étudiants de maitrise, 1978.

[4] Serge Mehl. *ChronoMath*. `http://chronomath.irem.univ-mrs.fr/` .

[5] Daniel Perrin. *Cours d'Algèbre*. Ellipses, 1996.

[6] Fritz Reinhardt et Heinrich Soeder. *Atlas des Mathématiques*. Le livre de Poche, 1997.